



## One Identity Manager 9.0

# Administrationshandbuch für die Datenarchivierung

**Copyright 2022 One Identity LLC.**

**ALLE RECHTE VORBEHALTEN.**

Diese Anleitung enthält urheberrechtlich geschützte Informationen. Die in dieser Anleitung beschriebene Software wird unter einer Softwarelizenz oder einer Geheimhaltungsvereinbarung bereitgestellt. Diese Software darf nur in Übereinstimmung mit den Bestimmungen der geltenden Vereinbarung verwendet oder kopiert werden. Kein Teil dieser Anleitung darf ohne die schriftliche Erlaubnis von One Identity LLC in irgendeiner Form oder mit irgendwelchen Mitteln, elektronisch oder mechanisch reproduziert oder übertragen werden, einschließlich Fotokopien und Aufzeichnungen für irgendeinen anderen Zweck als den persönlichen Gebrauch des Erwerbers.

Die Informationen in diesem Dokument werden in Verbindung mit One Identity Produkten bereitgestellt. Durch dieses Dokument oder im Zusammenhang mit dem Verkauf von One Identity LLC Produkten wird keine Lizenz, weder ausdrücklich oder stillschweigend, noch durch Duldung oder anderweitig, an jeglichem geistigen Eigentumsrecht eingeräumt. MIT AUSNAHME DER IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT GENANNTEN BEDINGUNGEN ÜBERNIMMT ONE IDENTITY KEINERLEI HAFTUNG UND SCHLIESST JEGLICHE AUSDRÜCKLICHE, IMPLIZIERTE ODER GESETZLICHE GEWÄHRLEISTUNG ODER GARANTIE IN BEZUG AUF IHRE PRODUKTE AUS, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE IMPLIZITE GEWÄHRLEISTUNG DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET ONE IDENTITY FÜR JEGLICHE DIREKTE, INDIREKTE, FOLGE-, STÖRUNGS-, SPEZIELLE ODER ZUFÄLLIGE SCHÄDEN (EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, SCHÄDEN FÜR VERLUST VON GEWINNEN, GESCHÄFTSUNTERBRECHUNGEN ODER VERLUST VON INFORMATIONEN), DIE AUS DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DIESES DOKUMENTS RESULTIEREN, SELBST WENN ONE IDENTITY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN HAT. One Identity übernimmt keinerlei Zusicherungen oder Garantien hinsichtlich der Richtigkeit und Vollständigkeit des Inhalts dieses Dokuments und behält sich das Recht vor, Änderungen an Spezifikationen und Produktbeschreibungen jederzeit ohne vorherige Ankündigung vorzunehmen. One Identity verpflichtet sich nicht, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Wenn Sie Fragen zu Ihrer potenziellen Nutzung dieses Materials haben, wenden Sie sich bitte an:

One Identity LLC.  
Attn: LEGAL Dept  
4 Polaris Way  
Aliso Viejo, CA 92656

Besuchen Sie unsere Website (<http://www.OneIdentity.com>) für regionale und internationale Büro-Adressen.


**Patente**

One Identity ist stolz auf seine fortschrittliche Technologie. Für dieses Produkt können Patente und anhängige Patente gelten. Für die aktuellsten Informationen über die geltenden Patente für dieses Produkt besuchen Sie bitte unsere Website unter <http://www.OneIdentity.com/legal/patents.aspx>.

**Marken**

One Identity und das One Identity Logo sind Marken und eingetragene Marken von One Identity LLC. in den USA und anderen Ländern. Für eine vollständige Liste der One Identity Marken besuchen Sie bitte unsere Website unter [www.OneIdentity.com/legal](http://www.OneIdentity.com/legal). Alle anderen Marken sind Eigentum der jeweiligen Besitzer.

**Legende**

 **WARNUNG:** Das Symbol **WARNUNG** weist auf ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.

 **VORSICHT:** Das Symbol **VORSICHT** weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.

# Inhalt

<b>Archivieren von Datenänderungen</b> .....	<b>4</b>
<b>Installieren einer One Identity Manager History Database</b> .....	<b>6</b>
<b>Bekanntgeben einer One Identity Manager History Database in der One Identity Manager-Datenbank</b> .....	<b>10</b>
Verbindung zur One Identity Manager History Database über Anwendungsserver herstellen .....	11
Direkte Verbindung zu einer One Identity Manager History Database herstellen .....	13
<b>Einrichten des Archivierungsverfahrens</b> .....	<b>15</b>
Auswahl des Archivierungsverfahrens in der One Identity Manager-Datenbank .....	16
Festlegen der Aufbewahrungszeiten .....	16
Archivieren der Änderungen in eine One Identity Manager History Database .....	19
Löschen der Aufzeichnungen ohne Archivierung .....	20
Performance-Optimierung zum Löschen von Aufzeichnungen .....	21
<b>Über uns</b> .....	<b>23</b>
Kontaktieren Sie uns .....	23
Technische Supportressourcen .....	23
<b>Index</b> .....	<b>24</b>

# Archivieren von Datenänderungen

Alle im One Identity Manager erfassten Datenänderungen werden zunächst in der One Identity Manager-Datenbank gespeichert. Die Aufzeichnungen sollten in regelmäßigen Abständen aus der One Identity Manager-Datenbank entfernt und in einer One Identity Manager History Database archiviert werden. Die One Identity Manager History Database stellt somit das Veränderungsarchiv dar. In der One Identity Manager History Database erfolgen statistische Auswertungen, die die Darstellungen von Trends oder Verläufen vereinfachen. Die Auswertung der historischen Daten erfolgt über die TimeTrace-Funktion oder über Berichte.

**HINWEIS:** Zur Auswertung historischer Daten im TimeTrace oder in Berichten können beliebig viele One Identity Manager History Databases verwendet werden. Dabei werden nicht nur One Identity Manager History Databases im aktuellen Format, sondern auch ältere Formate lesend unterstützt.

Die aufgezeichneten Daten unterliegen unter Umständen weiteren Regularien wie beispielsweise gesetzlichen Aufbewahrungsfristen. Es wird empfohlen One Identity Manager History Databases entsprechend der Berichtszeiträume zu betreiben. Nach Ablauf eines definierten Berichtszeitraums kann eine neue One Identity Manager History Database eingerichtet werden.

Abhängig vom Datenvolumen der One Identity Manager-Datenbank, den zu archivierenden Daten und deren Änderungshäufigkeit kann es erforderlich sein, in gewissen Zeitabständen (beispielsweise jährlich, quartalsweise oder monatlich) weitere One Identity Manager History Databases zu erstellen. Der Anteil der historisierten Daten am Gesamtvolumen einer One Identity Manager-Datenbank sollte maximal 25 % betragen. Anderenfalls kann es zu Performance-Problemen kommen.

Die Einrichtung einer One Identity Manager History Database umfasst folgende Schritte:

- Installieren der One Identity Manager History Database
- Bekanntgeben der One Identity Manager History Database in der One Identity Manager-Datenbank
- Einrichten des Archivierungsverfahrens

## Detaillierte Informationen zum Thema

- [Installieren einer One Identity Manager History Database auf Seite 6](#)
- [Bekanntgeben einer One Identity Manager History Database in der One Identity Manager-Datenbank auf Seite 10](#)
- [Einrichten des Archivierungsverfahrens auf Seite 15](#)

# Installieren einer One Identity Manager History Database

Die Installation einer One Identity Manager History Database ist ähnlich der Installation einer One Identity Manager-Datenbank. Ausführliche Informationen zu den Systemvoraussetzungen und zum Installieren einer Datenbank finden Sie *One Identity Manager Installationshandbuch*.

Die One Identity Manager History Database richten Sie mit dem Configuration Wizard ein.

**WICHTIG:** Starten Sie den Configuration Wizard immer auf einer administrativen Arbeitsstation.

## Um eine Datenbank im Configuration Wizard zu installieren

1. Starten Sie den Configuration Wizard.
2. Auf der Startseite des Configuration Wizard wählen Sie die Option **Datenbank erstellen und installieren** und klicken Sie **Weiter**.
3. Um eine neue Datenbank zu installieren, erfassen Sie auf der Seite **Administrative Datenbankverbindung herstellen** folgende Verbindungsdaten zur Datenbank.
  - **Server:** Datenbankserver.
  - (Optional) **Windows Authentifizierung:** Gibt an, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
  - **Nutzer:** SQL Server Anmeldename des Installationsbenutzer.
  - **Kennwort:** Kennwort für den Installationsbenutzer.

- ODER -

Um eine bestehende leere Datenbank zu verwenden, aktivieren Sie auf der Seite **Administrative Datenbankverbindung herstellen** die Option **Eine bereits existierende leere Datenbank verwenden** und erfassen Sie die Verbindungsdaten zur Datenbank.

- **Server:** Datenbankserver.
- (Optional) **Windows Authentifizierung:** Gibt an, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
- **Nutzer:** SQL Server Anmeldename des Installationsbenutzer.
- **Kennwort:** Kennwort für den Installationsbenutzer.
- **Datenbank:** Name der Datenbank.

**TIPP:** Um zusätzliche Verbindungsoptionen zu konfigurieren, aktivieren Sie die Option **Erweitert**.

4. Wenn Sie eine neue Datenbank erstellen, führen Sie auf der Seite **Datenbank erstellen** folgende Aktionen aus.
  - a. Erfassen Sie im Bereich **Datenbankeigenschaften** die folgenden Informationen zur Datenbank.

**Tabelle 1: Datenbankeigenschaften**

Eingabe	Beschreibung
Datenbankname	Name der Datenbank.
Datenverzeichnis	Verzeichnis, in dem die Datendatei erstellt wird. Zur Auswahl stehen: <ul style="list-style-type: none"> <li>• <b>&lt;Standard&gt;</b>: Standardverzeichnis des Datenbankservers.</li> <li>• <b>&lt;browse&gt;</b>: Wählen Sie ein Verzeichnis über den Dateibrowser.</li> <li>• <b>&lt;Verzeichnisangabe&gt;</b>: Verzeichnis, in dem bereits Datendateien installiert sind.</li> </ul>
Log Verzeichnis	Verzeichnis, in dem die Transaktionsprotokolldatei erstellt wird. Zur Auswahl stehen: <ul style="list-style-type: none"> <li>• <b>&lt;Standard&gt;</b>: Standardverzeichnis des Datenbankservers.</li> <li>• <b>&lt;browse&gt;</b>: Wählen Sie ein Verzeichnis über den Dateibrowser.</li> <li>• <b>&lt;Verzeichnisangabe&gt;</b>: Verzeichnis, in dem bereits Transaktionsprotokolldateien installiert sind.</li> </ul>
RAM-Tabellen Verzeichnis	Verzeichnis für Datendateigruppe und Datenbankdatei für speicheroptimierte Tabellen. Zur Auswahl stehen:

Eingabe	Beschreibung
Initiale Größe	<ul style="list-style-type: none"> <li>• <b>&lt;Standard&gt;</b>: Standardverzeichnis des Datenbankservers.</li> <li>• <b>&lt;browse&gt;</b>: Wählen Sie ein Verzeichnis über den Dateibrowser.</li> <li>• <b>&lt;Verzeichnisangabe&gt;</b>: Verzeichnis, in dem bereits Datendateien für speicheroptimierte Tabellen installiert sind.</li> </ul> <hr/> <p>Anfangsgröße der Datenbankdateien. Zur Auswahl stehen:</p> <ul style="list-style-type: none"> <li>• <b>&lt;Standard&gt;</b>: Standardvorgabe des Datenbankservers.</li> <li>• <b>&lt;custom&gt;</b>: Freie Eingabe.</li> <li>• Verschiedene empfohlene Größen: Abhängig von der Anzahl der Personen, die verwaltet werden.</li> </ul>

b. Wählen Sie im Bereich **Installationsquellen** das Verzeichnis mit den Installationsdateien.

- ODER -

Wenn Sie eine bestehende Datenbank verwenden, wählen Sie auf der Seite **Datenbank erstellen** im Bereich **Installationsquellen** das Verzeichnis mit den Installationsdateien.

5. Auf der Seite **Konfigurationsmodule auswählen** wählen Sie das Modul **Datenarchivierung**.
6. Auf der Seite **Verarbeitung der Datenbank** werden die Installationsschritte angezeigt.

Die Installation und Konfiguration der Datenbank wird durch den Configuration Wizard automatisch durchgeführt. Der Vorgang kann abhängig von der Systemperformance einige Zeit dauern. Nach Abschluss der Verarbeitung, klicken Sie **Weiter**.

**TIPP:** Um detaillierte Informationen zu den Verarbeitungsschritten und zum Migrationsprotokoll zu erhalten, aktivieren Sie die Option **Erweitert**.

7. Auf der letzten Seite des Configuration Wizard klicken Sie **Fertig**.

Nach der Schemainstallation sind weitere Schritte zur Konfiguration erforderlich.

- Geben Sie die One Identity Manager History Database in der One Identity Manager-Datenbank bekannt.
- Richten Sie in der One Identity Manager-Datenbank das Archivierungsverfahren ein.

**TIPP:** Alternativ können Sie die One Identity Manager History Database mit dem Kommandozeilenprogramm `Quantum.MigratorCmd.exe` erstellen.



#### Aufrufbeispiel:

```
quantum.migratorcmd.exe
```

```
  /Connection="Data Source=<Database server>;Initial Catalog=<Database>;User  
  ID=<Database user>;Password=<Password>"
```

```
  --Install
```

```
  /Module="HDB"
```

```
  /System=MSSQL
```

```
  /LogLevel= Info
```

```
  /Destination=<source folder>
```

Ausführliche Informationen zum Kommandozeilenprogramm Quantum.MigratorCmd.exe finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

#### Verwandte Themen

- [Bekanntgeben einer One Identity Manager History Database in der One Identity Manager-Datenbank](#) auf Seite 10
- [Einrichten des Archivierungsverfahrens](#) auf Seite 15

## Bekanntgeben einer One Identity Manager History Database in der One Identity Manager-Datenbank

Der Dienst One Identity Manager Service sorgt für die Datenübernahme aus der One Identity Manager-Datenbank in die One Identity Manager History Database. Für die Datenübernahme geben Sie die One Identity Manager History Database in der One Identity Manager-Datenbank im TimeTrace bekannt. Nutzen Sie den Designer um den Zugriff auf die One Identity Manager History Database einzurichten.

**HINWEIS:** Zur Auswertung historischer Daten im TimeTrace oder in Berichten können beliebig viele One Identity Manager History Databases verwendet werden. Dabei werden nicht nur One Identity Manager History Databases im aktuellen Format, sondern auch ältere Formate lesend unterstützt.

**HINWEIS:** Es kann immer nur eine One Identity Manager History Database als Ziel für die Datenübernahme verwendet werden, alle anderen Datenbanken sind nur lesend angebunden.

Um die Verbindung zu einer One Identity Manager History Database herzustellen haben Sie folgende Möglichkeiten:

- Variante 1: Erstellen Sie eine Verbindung zur One Identity Manager History Database über einen Anwendungsserver.

Diese Variante wird empfohlen. Nutzen Sie diese Variante für den Zugriff über eine verschlüsselte Verbindung zur One Identity Manager History Database. Weitere Informationen finden Sie unter [Verbindung zur One Identity Manager History Database über Anwendungsserver herstellen](#) auf Seite 11.

- Variante 2: Erstellen Sie eine direkte Verbindung zur One Identity Manager History Database.

Mit dieser Variante erfolgt der Zugriff auf die One Identity Manager History Database über eine unverschlüsselte Verbindung. Weitere Informationen finden Sie unter [Direkte Verbindung zu einer One Identity Manager History Database herstellen](#) auf Seite 13.

# Verbindung zur One Identity Manager History Database über Anwendungsserver herstellen

Für die Datenübernahme geben Sie die One Identity Manager History Database in der One Identity Manager-Datenbank im TimeTrace bekannt. Nutzen Sie den Designer um den Zugriff auf die One Identity Manager History Database einzurichten.

## Voraussetzungen für die Verbindung zu einer One Identity Manager History Database über einen Anwendungsserver

- Bei der Bekanntgabe der One Identity Manager History Database im TimeTrace wird eine Kennung verwendet.
- In der Konfigurationsdatei des Anwendungsserver (`web.config`) ist eine Kennung für die Verbindung zur One Identity Manager History Database eingetragen.
  - Erfassen Sie für jede One Identity Manager History Database eine eigene Kennung.
  - Die Kennungen müssen für alle Anwendungsserver eingetragen sein, über die sich ein Benutzer mit dem Manager anmelden kann.
  - Die Kennungen müssen für den Anwendungsserver eingetragen sein, über den sich der One Identity Manager Service verbindet.
- Die Anmeldung am Manager und am Web Portal erfolgt über einen Anwendungsserver. Andernfalls ist die Auswertung der Datenänderungen im TimeTrace oder in Berichten nicht möglich.
- Um Berichtabonnements und Berichte mit Datenänderungen zu generieren und per E-Mail zu versenden, ist ein Jobserver eingerichtet, der über einen Anwendungsserver arbeitet.

Ausführliche Informationen zum Einrichten eines Jobservers und zur Konfiguration des One Identity Manager Service finden Sie im *One Identity Manager Konfigurationshandbuch*.

## Um eine One Identity Manager History Database in den TimeTrace einzubinden

1. Melden Sie sich mit dem Designer an der One Identity Manager-Datenbank an.
2. Wählen Sie im Designer die Kategorie **Basisdaten > Allgemein > TimeTrace-Datenbanken**.
3. Wählen Sie den Menüeintrag **Objekt > Neu**.
4. Stellen Sie sicher, dass die Option **Kennung vom Anwendungsserver verwenden** aktiviert ist.
5. Erfassen Sie unter **Name der History-Datenbank** den Namen der One Identity Manager History Database.

6. Tragen Sie unter **Verbindungsparameter (lesen)** die Kennung für die Verbindung zur One Identity Manager History Database ein.

Die Kennung muss mit der Kennung in der Konfigurationsdatei des Anwendungsservers übereinstimmen.

7. Für die One Identity Manager History Database, in die die Daten aus der die One Identity Manager-Datenbank archiviert werden:
  - a. Aktivieren Sie die Option **Aktuelles Transportziel**.
  - b. Tragen Sie unter **Verbindungsparameter (transportieren)** die Verbindungsparameter für die Verbindung zur One Identity Manager History Database ein.
8. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

**HINWEIS:** Um die Verbindung zu einem späteren Zeitpunkt zu deaktivieren, setzen Sie die Option **Deaktiviert**. Ist eine One Identity Manager History Database deaktiviert, wird sie bei der Ermittlung der Änderungsinformationen im TimeTrace nicht berücksichtigt.

### **Um eine Kennung für die Verbindung zur One Identity Manager History Database im Anwendungsserver zu konfigurieren**

- Erfassen Sie bei der Installation eines Anwendungsservers die Kennung für die Verbindung zur One Identity Manager History Database.
- Um nachträglich eine One Identity Manager History Database anzubinden, tragen Sie in der Konfigurationsdatei des Anwendungsservers (`web.config`) in der Sektion `<connectionStrings>` die Kennung für die Verbindung ein.

#### **Beispiel:**

```
<connectionStrings>
    ...
    <add name="<Kennung für die History Database>"
        connectionString="Data Source=<Database server>;Initial
        Catalog=<Database name>;User ID=<Database
        user>;Password=<Password>" />
    ...
</connectionStrings>
```

#### **HINWEIS:**

Die Verbindungsinformationen in der Konfigurationsdatei des Anwendungsservers sind mittels Standard Microsoft ASP.NET Kryptographie verschlüsselt. Um die Verbindungsdaten nachträglich anzupassen, müssen Sie die Verbindungsinformationen zunächst entschlüsseln und nach der Änderung wieder verschlüsseln. Verwenden Sie

zum Entschlüsseln und Verschlüsseln das ASP.NET IIS-Registrierungstool (Aspnet\_regiis.exe).

Beispielaufrufe:

Entschlüsseln: aspnet\_regiis.exe -pdf connectionStrings <Pfad zur Webanwendung im IIS>

Verschlüsseln: aspnet\_regiis.exe -pef connectionStrings <Pfad zur Webanwendung im IIS>

## Verwandte Themen

- [Direkte Verbindung zu einer One Identity Manager History Database herstellen](#) auf Seite 13

# Direkte Verbindung zu einer One Identity Manager History Database herstellen

Für die Datenübernahme geben Sie die One Identity Manager History Database in der One Identity Manager-Datenbank im TimeTrace bekannt. Nutzen Sie den Designer um den Zugriff auf die One Identity Manager History Database einzurichten.

## **Um eine One Identity Manager History Database in den TimeTrace einzubinden**

1. Melden Sie sich mit dem Designer an der One Identity Manager-Datenbank an.
2. Wählen Sie im Designer die Kategorie **Basisdaten > Allgemein > TimeTrace-Datenbanken**.
3. Wählen Sie den Menüeintrag **Objekt > Neu**.
4. Stellen Sie sicher, dass die Option **Kennung vom Anwendungsserver verwenden** nicht aktiviert ist.
5. Erfassen Sie unter **Name der History-Datenbank** den Namen der One Identity Manager History Database.
6. Geben Sie die **Verbindungsparameter (lesen)** bekannt.
  - a. Öffnen Sie den Eingabedialog für die Verbindungsdaten über die Schaltfläche [...] neben dem Eingabefeld.
  - b. Geben Sie die Verbindungsdaten zur One Identity Manager History Database an.
    - **Server:** Datenbankserver.
    - (Optional) **Windows Authentifizierung:** Gibt an, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser

Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.

- **Nutzer:** SQL Server Anmeldename des Benutzer.
  - **Kennwort:** Kennwort für die SQL Server Anmeldung des Benutzer.
  - **Datenbank:** Wählen Sie die Datenbank.
7. Für die One Identity Manager History Database, in die die Daten aus der die One Identity Manager-Datenbank archiviert werden:
    - a. Aktivieren Sie die Option **Aktuelles Transportziel**.
    - b. Tragen Sie unter **Verbindungsparameter (transportieren)** die Verbindungsparameter für die Verbindung zur One Identity Manager History Database ein.
  8. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

**HINWEIS:** Um die Verbindung zu einem späteren Zeitpunkt zu deaktivieren, setzen Sie die Option **Deaktiviert**. Ist eine One Identity Manager History Database deaktiviert, wird sie bei der Ermittlung der Änderungsinformationen im TimeTrace nicht berücksichtigt.

## Verwandte Themen

- [Verbindung zur One Identity Manager History Database über Anwendungsserver herstellen](#) auf Seite 11

## Einrichten des Archivierungsverfahrens

Alle im One Identity Manager protokollierten Aufzeichnungen werden zunächst in der One Identity Manager-Datenbank gespeichert. Der Anteil der historisierten Daten am Gesamtvolumen einer One Identity Manager-Datenbank sollte maximal 25 % betragen. Anderenfalls kann es zu Performance-Problemen kommen. Die Aufzeichnungen sollten in regelmäßigen Abständen aus der One Identity Manager-Datenbank entfernt und archiviert werden.

Um die aufgezeichneten Daten in regelmäßigen Abständen aus der One Identity Manager-Datenbank zu entfernen, werden folgende Verfahren angeboten:

- Die Daten können direkt aus der One Identity Manager-Datenbank in eine One Identity Manager History Database übernommen werden. Dieses ist das Standardverfahren für die Datenarchivierung. Wählen Sie dieses Verfahren, wenn die Server auf denen die One Identity Manager-Datenbank und die One Identity Manager History Database liegen, einander sehen.
- Die Daten werden ohne Archivierung nach einer festgelegten Zeitspanne aus der One Identity Manager-Datenbank gelöscht.

Für die direkte Übernahme in eine One Identity Manager History Database werden in der One Identity Manager-Datenbank alle Aufzeichnungen, die von einer Aktion ausgelöst wurden, anhand einer ID-Nummer, der GenProcID, zu einer Prozessgruppe zusammengefasst. Nach erfolgreichem Export werden die exportierten Prozessgruppen mit den zugehörigen Aufzeichnungen aus der One Identity Manager-Datenbank gelöscht.

Für die direkte Übernahme in eine One Identity Manager History Database müssen folgende Bedingungen erfüllt sein:

- Der Teilbereich der Aufzeichnungen ist für den Export konfiguriert.
- Die Aufbewahrungszeit aller Aufzeichnungen, die zu einer Prozessgruppe gehören, ist abgelaufen, unabhängig davon ob der Teilbereich zum Export gekennzeichnet ist.
- Es gibt keine aktiven Prozesse mit der GenProcID der Prozessgruppe in der DBQueue, in der Jobqueue oder als geplante Operationen.
- Es gibt für die auslösende Aktion mindestens eine Aufzeichnung in dem Teilbereich, der exportiert werden soll.

# Auswahl des Archivierungsverfahrens in der One Identity Manager-Datenbank

Die Auswahl des grundlegenden Verfahrens treffen Sie über die Einstellung des Konfigurationsparameters **Common | ProcessState | ExportPolicy**. Passen Sie den Konfigurationsparameter im Designer an.

- Ist der Konfigurationsparameter deaktiviert, verbleiben die Daten in der One Identity Manager-Datenbank.
- Ist der Konfigurationsparameter aktiviert, dann wird das gewählte Verfahren angewendet.
  - **HDB**: Die Daten werden nach Ablauf einer festgelegten Zeitspanne direkt in eine One Identity Manager History Database übernommen.
  - **NONE**: Die Daten werden nach Ablauf einer festgelegten Zeitspanne aus der One Identity Manager-Datenbank gelöscht.

Für jeden Teilbereich der Aufzeichnungen können Sie nach der Auswahl des grundlegenden Verfahrens separat festlegen, ob die Daten exportiert oder gelöscht werden. Die Festlegung für die einzelnen Bereiche treffen Sie über Konfigurationsparameter. Passen Sie die Konfigurationsparameter im Designer an.

**Tabelle 2: Konfigurationsparameter für die Behandlung der aufgezeichneten Informationen**

Konfigurationsparameter	Bedeutung
Common   ProcessState   PropertyLog   IsToExport	Die aufgezeichneten Datenänderungen sollen exportiert werden. Ist der Konfigurationsparameter nicht aktiv, werden die Informationen nach Ablauf der Aufbewahrungszeit gelöscht.
Common   ProcessState   ProgressView   IsToExport	Die Prozessinformationen sollen exportiert werden. Ist der Konfigurationsparameter nicht aktiv, werden die Informationen nach Ablauf der Aufbewahrungszeit gelöscht.
Common   ProcessState   JobHistory   IsToExport	Die Informationen in der Prozesshistorie sollen exportiert werden. Ist der Konfigurationsparameter nicht aktiv, werden die Informationen nach Ablauf der Aufbewahrungszeit gelöscht.

## Festlegen der Aufbewahrungszeiten

Die Aufzeichnungen werden, abhängig vom gewählten Archivierungsverfahren, nach Ablauf der Aufbewahrungszeiten aus der One Identity Manager-Datenbank exportiert oder



gelöscht. Für die Teilbereiche, deren Aufzeichnungen exportiert werden, sollte eine längere Aufbewahrungszeit gewählt werden, als für die Teilbereiche, deren Aufzeichnungen gelöscht werden.

Die Aufzeichnungen werden erst exportiert, wenn die Aufbewahrungszeiten aller Teilbereiche abgelaufen ist und keine weiteren aktiven Prozesse für die Prozessgruppe (GenProcID) in der DBQueue, der Prozesshistorie oder als geplante Operation existieren.

**HINWEIS:** Wenn Sie keine Aufbewahrungszeiten festlegen, werden die Aufzeichnungen dieser Teilbereiche täglich innerhalb der tägliche Wartungsaufträge des DBQueue Prozessors aus der One Identity Manager-Datenbank gelöscht.

Die Aufbewahrungszeiten für die einzelnen Bereiche legen Sie über Konfigurationsparameter fest. Passen Sie den Konfigurationsparameter im Designer an.

**Tabelle 3: Konfigurationsparameter für die Aufbewahrungszeiten**

Konfigurationsparameter	Bedeutung
Common   ProcessState   PropertyLog   LifeTime	Mit diesem Konfigurationsparameter wird die maximale Aufbewahrungszeit für aufgezeichnete Datenänderungen in der Datenbank festgelegt.
Common   ProcessState   ProgressView   LifeTime	Mit diesem Konfigurationsparameter wird die maximale Aufbewahrungszeit für Prozessinformationen in der Datenbank festgelegt.
Common   ProcessState   JobHistory   LifeTime	Mit diesem Konfigurationsparameter wird die maximale Aufbewahrungszeit für Aufzeichnungen aus der Prozesshistorie in der Datenbank festgelegt.

**Beispiel 1:**

Die Aufzeichnungen werden direkt in eine One Identity Manager History Database übernommen. Für die einzelnen Teilbereiche wurden folgende Konfigurationen gewählt:

Konfiguration	Prozess- informationen	Prozess- historie	Daten- änderungen
Daten exportieren	Nein	Nein	Ja
Aufbe- wahrungszeit	3 Tage	4 Tage	5 Tage

Daraus ergibt sich folgender Ablauf:

<b>Zeitpunkt</b>	<b>Prozessinformationen</b>	<b>Prozesshistorie</b>	<b>Datenänderungen</b>
Tag 3	Daten werden in der One Identity Manager-Datenbank gelöscht.	Keine Aktion.	Keine Aktion.
Tag 4	-	Daten werden in der One Identity Manager-Datenbank gelöscht.	Keine Aktion.
Tag 5	-	-	Daten werden in die One Identity Manager History Database übernommen und anschließend in der One Identity Manager-Datenbank gelöscht.

### Beispiel 2:

Die Aufzeichnungen werden direkt in eine One Identity Manager History Database übernommen. Für die einzelnen Teilbereiche wurden folgende Konfigurationen gewählt:

<b>Konfiguration</b>	<b>Prozessinformationen</b>	<b>Prozesshistorie</b>	<b>Datenänderungen</b>
Daten exportieren	Ja	Nein	Ja
Aufbewahrungszeit	3 Tage	4 Tage	5 Tage

Daraus ergibt sich folgender Ablauf:

<b>Zeitpunkt</b>	<b>Prozessinformationen</b>	<b>Prozesshistorie</b>	<b>Datenänderungen</b>
Tag 3	Keine Aktion, da die Aufbewahrungszeit noch nicht in allen Teilbe-	Keine Aktion.	Keine Aktion.

Zeitpunkt	Prozessinformationen	Prozesshistorie	Datenänderungen
	reichen abgelaufen ist.		
Tag 4	Keine Aktion, da die Aufbewahrungszeit noch nicht in allen Teilbereichen abgelaufen ist.	Daten werden in der One Identity Manager-Datenbank gelöscht.	Keine Aktion.
Tag 5	Daten werden exportiert und anschließend gelöscht.	-	Daten werden in die One Identity Manager History Database übernommen und anschließend in der One Identity Manager-Datenbank gelöscht.

## Archivieren der Änderungen in eine One Identity Manager History Database

Die Daten können direkt aus der One Identity Manager-Datenbank in eine One Identity Manager History Database übernommen werden. Dieses ist das Standardverfahren für die Datenarchivierung.

Um dieses Verfahren zu nutzen, nehmen Sie in der One Identity Manager-Datenbank folgende Konfigurationseinstellungen vor:

- Aktivieren Sie im Designer den Konfigurationsparameter **Common | ProcessState | ExportPolicy** und tragen Sie den Wert **HDB** ein.
- Konfigurieren Sie die Teilbereiche für den Export und legen Sie die Aufbewahrungszeiten fest.
- Prüfen Sie im Designer den Wert der Konfigurationsparameters **Common | ProcessState | PackageSizeHDB**. Dieser Parameter legt die maximale Anzahl der Prozessgruppen fest, die in die One Identity Manager History Database übertragen werden. Der Standardwert ist **10000**.
- Stellen Sie sicher, dass der Zeitplan **Transport in die History Database** aktiviert ist.

Der Zeitplan sorgt für die Übertragung der Daten aus der One Identity Manager-Datenbank in die One Identity Manager History Database. Der Zeitplan ist im Standard auf ein Ausführungsintervall von **6** Stunden eingestellt. Passen Sie im Designer das Ausführungsintervall bei Bedarf an.

## Verwandte Themen

- [Auswahl des Archivierungsverfahrens in der One Identity Manager-Datenbank auf Seite 16](#)
- [Festlegen der Aufbewahrungszeiten auf Seite 16](#)
- [Bekanntgeben einer One Identity Manager History Database in der One Identity Manager-Datenbank auf Seite 10](#)

# Löschen der Aufzeichnungen ohne Archivierung

Sollen die Aufzeichnungen einzelner Teilbereiche für einen gewissen Zeitraum in der One Identity Manager-Datenbank gehalten werden, jedoch keine spätere Archivierung erfolgen, dann haben Sie folgende Möglichkeiten:

- Um einen einzelnen Teilbereich von der Archivierung auszuschließen, konfigurieren Sie diesen Teilbereich nicht für den Export, sondern legen nur den Aufbewahrungszeitraum fest.
- Um alle Teilbereiche ohne Archivierung direkt zu löschen, legen Sie die Aufbewahrungszeiten fest. Aktivieren Sie im Designer den Konfigurationsparameter **Common | ProcessState | ExportPolicy** und tragen Sie den Wert **NONE** ein.

Die Aufzeichnungen werden nach Ablauf der Aufbewahrungszeit durch den DBQueue Prozessor aus der One Identity Manager-Datenbank gelöscht. Zusätzlich werden alle Einträge für ausgelöste Aktionen gelöscht, zu denen es keine Aufzeichnungen in den Teilbereichen gibt.

**HINWEIS:** Wenn Sie keine Aufbewahrungszeiten festlegen, werden die Aufzeichnungen dieser Teilbereiche innerhalb der täglichen Wartungsaufträge des DBQueue Prozessor aus der One Identity Manager-Datenbank gelöscht.

## Verwandte Themen

- [Auswahl des Archivierungsverfahrens in der One Identity Manager-Datenbank auf Seite 16](#)
- [Festlegen der Aufbewahrungszeiten auf Seite 16](#)
- [Performance-Optimierung zum Löschen von Aufzeichnungen auf Seite 21](#)

# Performance-Optimierung zum Löschen von Aufzeichnungen

Bei großen Datenmengen können Sie zur Performance-Optimierung die Menge der zu löschenden Objekte pro Operation und Verarbeitungslauf des DBQueue Prozessor festlegen. Die Festlegung für die einzelnen Bereiche treffen Sie über Konfigurationsparameter.

**Tabelle 4: Konfigurationsparameter für das Löschen der aufgezeichneten Datenänderungen**

Konfigurationsparameter	Bedeutung
Common   ProcessState   PropertyLog   Delete	Erlaubt die Konfiguration des Löschverhaltens für aufgezeichnete Datenänderungen.
Common   ProcessState   PropertyLog   Delete   BulkCount	Anzahl der Einträge, die in einer Operation gelöscht werden sollen. Standardwert ist <b>200</b> .
Common   ProcessState   PropertyLog   Delete   TotalCount	Gesamtmenge der Einträge, die in einem Verarbeitungslauf gelöscht werden sollen. Standardwert ist <b>10000</b> .

**Tabelle 5: Konfigurationsparameter für das Löschen der Prozessinformationen**

Konfigurationsparameter	Bedeutung
Common   ProcessState   ProgressView   Delete	Erlaubt die Konfiguration des Löschverhaltens für Prozessinformationen.
Common   ProcessState   ProgressView   Delete   BulkCount	Anzahl der Einträge, die in einer Operation gelöscht werden sollen. Standardwert ist <b>200</b> .
Common   ProcessState   ProgressView   Delete   TotalCount	Gesamtmenge der Einträge, die in einem Verarbeitungslauf gelöscht werden sollen. Standardwert ist <b>10000</b> .

**Tabelle 6: Konfigurationsparameter für das Löschen der Prozesshistorie**

Konfigurationsparameter	Bedeutung
Common   ProcessState   JobHistory   Delete	Erlaubt die Konfiguration des Löschverhaltens für die Prozesshistorie.
Common   ProcessState   JobHistory   Delete   BulkCount	Anzahl der Einträge, die in einer Operation gelöscht werden sollen. Standardwert ist <b>200</b> .

Konfigurationsparameter	Bedeutung
Common   ProcessState   JobHistory   Delete   TotalCount	Gesamtmenge der Einträge, die in einem Verarbeitungslauf gelöscht werden sollen. Standardwert ist <b>10000</b> .

**Tabelle 7: Konfigurationsparameter für das Löschen von Prozessstatus-Einträge**

Konfigurationsparameter	Bedeutung
Common   ProcessState   Delete	Erlaubt die Konfiguration des Löschverhaltens für die Einträge zum Prozessstatus.
Common   ProcessState   Delete   BulkCount	Anzahl der Einträge, die in einer Operation gelöscht werden sollen. Standardwert ist <b>500</b> .
Common   ProcessState   Delete   TotalCount	Gesamtmenge der Einträge, die in einem Verarbeitungslauf gelöscht werden sollen. Standardwert ist <b>10000</b> .

One Identity Lösungen eliminieren die Komplexität und die zeitaufwendigen Prozesse, die häufig bei der Identity Governance, der Verwaltung privilegierter Konten und dem Zugriffsmanagement aufkommen. Unsere Lösungen fördern die Geschäftsagilität und bieten durch lokale, hybride und Cloud-Umgebungen eine Möglichkeit zur Bewältigung Ihrer Herausforderungen beim Identitäts- und Zugriffsmanagement.

## Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen, wie Lizenzierungen, Support oder Support-Erneuerungen, besuchen Sie <https://www.oneidentity.com/company/contact-us.aspx>.

## Technische Supportressourcen

Technische Unterstützung steht für One Identity Kunden mit einem gültigen Wartungsvertrag und Kunden mit Testversionen zur Verfügung. Sie können auf das Support Portal unter <https://support.oneidentity.com/> zugreifen.

Das Support Portal bietet Selbsthilfe-Tools, die Sie verwenden können, um Probleme schnell und unabhängig zu lösen, 24 Stunden am Tag, 365 Tage im Jahr. Das Support Portal ermöglicht Ihnen:

- Senden und Verwalten von Serviceanfragen
- Anzeigen von Knowledge Base Artikeln
- Anmeldung für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Videos unter [www.YouTube.com/OneIdentity](http://www.YouTube.com/OneIdentity)
- Engagement in der One Identity Community
- Chat mit Support-Ingenieuren
- Anzeigen von Diensten, die Sie bei Ihrem Produkt unterstützen

## D

Datenänderung

Aufbewahrungszeit 16

## O

One Identity Manager History Database

Archivierungsverfahren 15-16

Datenarchivierung 4, 15-16

konfigurieren 19

Quelldatenbank 10-11, 13

## P

Prozesshistorie

Aufbewahrungszeit 16

Prozessinformation

archivieren 16

Ausbewahrungszeit 16

exportieren 19

importieren 19

löschen 20

Prozessüberwachung

archivieren 15

Aufbewahrungszeit 16